UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,477	07/14/2004	James E. Aston	014682.000010	4476

44870 7590 01/25/2007

MOORE & VAN ALLEN, PLLC For IBM
P.O. Box 13706
Research Triangle Park, NC 27709

EXAMINER	
DWIVEDI, MAHESH H	
ART UNIT	**PAPER NUMBER**
2168	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/710,477	ASTON ET AL.	
	Examiner	Art Unit	
	Mahesh H. Dwivedi	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Receipt of Applicant's Amendment, filed on 11/08/2006, is acknowledged. The amendment includes amending the specification and amending claims 1, 9, 13, 21, 30, and 38.

Specification

2. The objections raised in the office action mailed on 08/10/2006 have been overcome by the applicant amendments received on 11/08/2006.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by **Mclchionc** (U.S. Patent 6,973,578).

5. Regarding claim 1, **Mclchionc** teaches a method comprising:

A) allowing one of a highest security level, a middle security level and a lowest security level to be set (Column 2, lines 29-33, Column 4, lines 62-67-Column 5, lines 1-2, Column 6, lines 55-65);

B) flagging a program as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append

operation with the local file and the highest security level being set (Column 3, lines 56-67-Column 4, lines 1-9, Column 4, lines 62-67-Column 5, lines 1-18);

C) the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system and at least the medium security level being set (Column 3, lines 56-67-Column 4, lines 1-9);

D) the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system and at least the lowest security level being set (Column 3, lines 56-67-Column 4, lines 1-9); and

E) the program attempting to write or append a remote file to the local file system and at least the medium security level being set (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"allowing one of a highest security level, a middle security level and a lowest security level to be set"** as "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30) and "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system…It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65).

The examiner further notes that Table 1 of **McIchionc** clearly shows differing levels of security (see first through fourth) applied to a system. The examiner further notes that **McIchionc** teaches **"flagging a program as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file and the highest security level being set"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the

files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9) and "In order to facilitate the selection of the appropriate virus detection actions, each process may have an associated risk level identifier associated therewith...the process may be identified by...a method in which files are being accessed by the process (opened for read, opened for write, execution, etc.)" (Column 4, lines 62-67-Column 5, lines 1-13). The examiner further notes that **McIchionc** teaches **"the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system and at least the medium security level being set"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system and at least the lowest security level being set"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the program attempting to write or append a remote file to the local file system and at least the medium security level being set"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 2, 6, 8-9, 13-16, 21, 23-25, 28, 30, 32-34, 38, and 40-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Norton** (Article entitled "Norton AntiVirus Corporate Edition User's Guide, dated 09/11/2001).

8. Regarding claim 2, **McIchionc** does not explicitly teach a method comprising:
A) inhibiting a write or append operation associated with program in response to flagging the program.

Norton, however, teaches **"inhibiting a write or append operation associated with program in response to flagging the program"** as "By default, when a virus is detected by either Realtime Protection or during a scan, Norton AntiVirus attempts to clean the virus from the infected file" (Page 13, Section: "What to do if a virus is detected").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect

viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 6, **McIchionc** does not explicitly teach a method comprising: A) storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program.

Norton, however, teaches **"storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 8, **McIchionc** does not explicitly teach a method comprising: A) logging any file system operations including recording a filename and a location where the local or shared file is written.

Norton, however, teaches **"logging any file system operations including recording a filename and a location where the local or shared file is written"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the

name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 9, **McIchionc** teaches a method comprising:

A) allowing a security level to be set (Column 2, lines 29-33, Column 4, lines 62-67-Column 5, lines 1-2, Column 6, lines 55-65);

B) monitoring predetermined file system operations associated with a program (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"allowing a security level to be set"** as "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30) and "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system…It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65). The examiner further notes that Table 1 of **McIchionc** clearly shows differing levels of security (see first through fourth) applied to a system. The examiner further notes that **McIchionc** teaches **"monitoring predetermined file system operations associated with a program"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files,

moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Mclchionc does not explicitly teach:

C) logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written.

Norton, however, teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **Mclchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 13, **Mclchionc** does not explicitly teach a method comprising:

A) following a predefined procedure in response to the level of security set.

Norton, however, teaches **"following a predefined procedure in response to the level of security set"** as "If you regularly scan the same set of files or folders you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus-free" (Page 31, Section: Configuring Custom Scans").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Norton's would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 14, **McIchionc** further teaches a method comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 15, **McIchionc** further teaches a method comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file (Column 3, lines 56-67-Column 4, lines 1-9);

B) the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system (Column 3, lines 56-67-Column 4, lines 1-9);

C) the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system (Column 3, lines 56-67-Column 4, lines 1-9); and

D) the program attempting to write or append a remote file to the local file system (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"flagging the program in response to at least one of: the program opening a local file on a local file**

system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file" as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the program attempting to write or append a remote file to the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 16, **McIchionc** does not explicitly teach a method comprising: A) inhibiting any predetermined file system operations associated with the program in response to the program being flagged.

Norton, however, teaches **"inhibiting any predetermined file system operations associated with the program in response to the program being flagged"** as "By default, when a virus is detected by either Realtime Protection or during a scan, Norton AntiVirus attempts to clean the virus from the infected file" (Page 13, Section: "What to do if a virus is detected").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 21, **McIchionc** teaches a system comprising:

A) a file system protection program including: means to monitor predetermined file system operations associated with another program (Column 3, lines 56-67-Column 4, lines 1-9).

B) a plurality of settable levels of security (Column 2, lines 29-33, Column 4, lines 62-67-Column 5, lines 1-2, Column 6, lines 55-65);

The examiner notes that **McIchionc** teaches **"a file system protection program including: means to monitor predetermined file system operations associated with another program"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"a plurality of settable levels of security"** as "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30) and "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system…It should be noted that the number of

categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65).

Mclchionc does not explicitly teach:

C) a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security; and

D) means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written.

Norton, however, teaches "**a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security**" as "If you regularly scan the same set of files or folders you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus-free" (Page 31, Section: Configuring Custom Scans") and "**means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written**" as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **Mclchionc's** to provide a method to quickly detect

viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 23, **McIchionc** does not explicitly teach a system comprising:
A) a log to record any predetermined file system operations.

Norton, however, teaches **"a log to record any predetermined file system operations"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 24, **McIchionc** further teaches a system comprising:
A) means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file (Column 3, lines 56-67-Column 4, lines 1-9);
B) the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system (Column 3, lines 56-67-Column 4, lines 1-9);

C) the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system (Column 3, lines 56-67-Column 4, lines 1-9); and
D) the other program attempting to write or append a remote file to the local file system (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the other program attempting to write or append a remote file to the local file system"** as "an indication is first received that a file is being accessed by a process...such accessing may include

opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 25, **McIchionc** further teaches a system comprising:
A) means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 28, **McIchionc** does not explicitly teach a system comprising:
A) to inhibit predetermined file system operations associated with the other program in response to the program other being flagged.

Norton, however, teaches **"to inhibit predetermined file system operations associated with the other program in response to the program other being flagged"** as "By default, when a virus is detected by either Realtime Protection or during a scan, Norton AntiVirus attempts to clean the virus from the infected file" (Page 13, Section: "What to do if a virus is detected").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 30, **McIchionc** teaches a method comprising:

A) providing a file system protection program including: providing means to monitor predetermined file system operations associated with another program (Column 3, lines 56-67-Column 4, lines 1-9).

B) defining a plurality of settable levels of security (Column 2, lines 29-33, Column 4, lines 62-67-Column 5, lines 1-2, Column 6, lines 55-65).

The examiner notes that **McIchionc** teaches **"providing a file system protection program including: providing means to monitor predetermined file system operations associated with another program"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"defining a plurality of settable levels of security"** as "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30) and "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system…It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65).

McIchionc does not explicitly teach:

C) providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security; and

D) providing means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written.

Norton, however, teaches **"providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a**

particular file system operation also associated with the currently set level of security" as "If you regularly scan the same set of files or folders you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus-free" (Page 31, Section: Configuring Custom Scans") and **"providing means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 32, **McIchionc** does not explicitly teach a method comprising:

A) forming a log to record any predetermined file system operations.

Norton, however, teaches **"forming a log to record any predetermined file system operations"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 33, **McIchionc** further teaches a method comprising:

A) providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file (Column 3, lines 56-67-Column 4, lines 1-9);

B) the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system (Column 3, lines 56-67-Column 4, lines 1-9);

C) the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system (Column 3, lines 56-67-Column 4, lines 1-9); and

D) the other program attempting to write or append a remote file to the local file system (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The

examiner further notes that **McIchionc** teaches **"the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **McIchionc** teaches **"the other program attempting to write or append a remote file to the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 34, **McIchionc** further teaches a method comprising:

A) providing means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"providing means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files,

moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 38, **McIchionc** teaches a computer-readable medium comprising:

A) allowing a security level to be set (Column 2, lines 29-33, Column 4, lines 62-67-Column 5, lines 1-2, Column 6, lines 55-65);

B) monitoring predetermined file system operations associated with a program (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"allowing a security level to be set"** as "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30) and "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system…It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65). The examiner further notes that Table 1 of **McIchionc** clearly shows differing levels of security (see first through fourth) applied to a system. The examiner notes that **McIchionc** teaches **"monitoring predetermined file system operations associated with a program"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

McIchionc does not explicitly teach:

C) logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written.

Norton, however, teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written"** as "Depending on your anti-virus policy, you can

change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 13, **McIchionc** does not explicitly teach a computer-readable medium comprising:

A) following a predefined procedure in response to a level of security set.

Norton, however, teaches **"following a predefined procedure in response to a level of security set"** as "If you regularly scan the same set of files or folders you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus-free"" (Page 32, Section: Configuring Custom Scans").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

Regarding claim 41, **McIchionc** further teaches a computer-readable medium comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 42, **McIchionc** further teaches a computer-readable medium comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file (Column 3, lines 56-67-Column 4, lines 1-9);

B) the program reading or opening itself and the program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system (Column 3, lines 56-67-Column 4, lines 1-9);

C) the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system (Column 3, lines 56-67-Column 4, lines 1-9); and

D) the program attempting to write or append a remote file to the local file system (Column 3, lines 56-67-Column 4, lines 1-9).

The examiner notes that **McIchionc** teaches **"flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file"** as "an indication is first received that a file is being accessed by a process...such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the

files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **Mclchionc** teaches **"the program reading or opening itself and the program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **Mclchionc** teaches **"the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9). The examiner further notes that **Mclchionc** teaches **"the program attempting to write or append a remote file to the local file system"** as "an indication is first received that a file is being accessed by a process…such accessing may include opening the files, reading the files, executing the files, indexing the files, organizing the files, editing the files, moving the files, or any other function that involves the files" (Column 3, lines 58-67-Column 4,lines 1-9).

Regarding claim 43, **Mclchionc** does not explicitly teach a computer-readable medium comprising:

A) inhibiting any predetermined file system operations associated with the program in response to the program being flagged.

Norton, however, teaches **"inhibiting any predetermined file system operations associated with the program in response to the program being flagged"** as "By default, when a virus is detected by either Realtime Protection or

during a scan, Norton AntiVirus attempts to clean the virus from the infected file" (Page 13, Section: "What to do if a virus is detected").

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

9. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Satterlee et al.** (U.S. PGPUB 2004/0025015).

10. Regarding claim 3, **McIchionc** does not explicitly teach a method comprising: A) monitoring all file operations associated with the program in response to the program not being in a safe list.

Satterlee, however, teaches **"monitoring all file operations associated with the program in response to the program not being in a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 4, **McIchionc** does not explicitly teach a method comprising:

A) permitting selected read and write operations in response to a predefined rules table.

Satterlee, however, teaches **"permitting selected read and write operations in response to a predefined rules table"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Mclchionc's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 5, **Mclchionc** does not explicitly teach a method comprising:

A) sending an alert in response to flagging the program.

Satterlee, however, teaches **"sending an alert in response to flagging the program"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Mclchionc's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an

harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

11. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Wolff et al.** (U.S. PGPUB 2002/0174358).

12. Regarding claim 7, **McIchionc** does not explicitly teach a method comprising:

A) sending an alert to a network monitoring system in response to flagging the program.

Wolff, however, teaches **"sending an alert to a network monitoring system in response to flagging the program"** as "An event report, such as a virus detection event, is sent from a reporting computer 2 to a receiving computer 6 via an internet link 4" (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Wolff's** would have allowed **McIchionc's** to provide a method to allow major antivirus software providers to accurately determine what viruses are common and attacking how many users in order to direct resources to combat these viruses, as noted by **Wolff** (Paragraph 4).

13. Claims 10-12, 17, 19-20, 22, 26, 29, 31, 35, 37, 39, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Norton** (Article entitled "Norton AntiVirus Corporate Edition User's Guide, dated 09/11/2001) as applied to claims 2, 6, 8-9, 13-16, 21, 23-25, 28, 30, 32-34, 38, and 40-43 and further in view of **Satterlee et al.** (U.S. PGPUB 2004/0025015).

14. Regarding claim 10, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) selecting the program for monitoring in response to the program not being on a safe list.

Satterlee, however, teaches **"selecting the program for monitoring in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 11, **McIchionc** does not explicitly teach a method comprising:

A) logging any file system operations.

Norton, however, teaches **"logging any file system operations"** as "Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only)" (Page 13, Section: "What to do if a virus is detected") and "If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected" (Page 32, Section: Interpreting scan results").

The examiner notes that the dialog box on page 32 contains the location of the infected file as a path.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Norton's** would have allowed **McIchionc's** to provide a method to quickly detect

viruses in order to remove them from a computer so that the virus cannot spread to other files and cause damage, as noted by **Norton** (Page 8).

McIchionc and **Norton** do not explicitly teach:

B) associated with any programs on the safe list.

Satterlee, however, teaches **"associated with any programs on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 12, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) receiving a notification that the program intends to perform one of the predetermined file system operations.

Satterlee, however, teaches **"receiving a notification that the program intends to perform one of the predetermined file system operations"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to

allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 17, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations.

Satterlee, however, teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 19, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) presenting an alert to a user for approval before the predetermined file system operation is performed by the program.

Satterlee, however, teaches **"presenting an alert to a user for approval before the predetermined file system operation is performed by the program"** as "in step 605 the protector application 115 will consult the database 110 to determine if the user has been previously queried about the new non-validated executable file…If the user has previously approved the loading of this executable file in step 610, or if the

user approves the new executable in this instance in step 615, then execution of the executable file will proceed" (Paragraph 45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 20, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) requiring approval before performing any predetermined file system operations associated the program in response to the program not being on a safe list.

Satterlee, however, teaches **"requiring approval before performing any predetermined file system operations associated the program in response to the program not being on a safe list"** as "in step 605 the protector application 115 will consult the database 110 to determine if the user has been previously queried about the new non-validated executable file…If the user has previously approved the loading of this executable file in step 610, or if the user approves the new executable in this instance in step 615, then execution of the executable file will proceed" (Paragraph 45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 22, **McIchionc** and **Norton** do not explicitly teach a system comprising:

A) a safe list; and

B) wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list.

Satterlee, however, teaches **"a safe list"** as "predetermined list of approved programs" (Paragraph 13) and **"wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 26, **McIchionc** and **Norton** do not explicitly teach a system comprising:

A) means to send an alert in response to flagging the other program.

Satterlee, however, teaches **"means to send an alert in response to flagging the other program"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or

network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 29, **Mclchionc** and **Norton** do not explicitly teach a system comprising:

A) means to present an alert to a user; and

B) means for the user to approve the one of the predetermined file system operations before being performed by the other program.

Satterlee, however, teaches **"means to present an alert to a user"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39), and **"means for the user to approve the one of the predetermined file system operations before being performed by the other program"** as "in step 605 the protector application 115 will consult the database 110 to determine if the user has been previously queried about the new non-validated executable file…If the user has previously approved the loading of this executable file in step 610, or if the user approves the new executable in this instance in step 615, then execution of the executable file will proceed" (Paragraph 45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Mclchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 31, **Mclchionc** and **Norton** do not explicitly teach a system comprising:

A) providing a safe list; and

B) adapting the file system protection program to monitor the other program in response to the other program not being on the safe list.

Satterlee, however, teaches **"providing a safe list"** as "predetermined list of approved programs" (Paragraph 13) and **"adapting the file system protection program to monitor the other program in response to the other program not being on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 35, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) providing means to send an alert in response to flagging the other program.

Satterlee, however, teaches **"providing means to send an alert in response to flagging the other program"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or

network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 37, **McIchionc** and **Norton** do not explicitly teach a method comprising:

A) providing means to present an alert to a user; and

B) providing means for the user to approve the one of the predetermined file system operations before being performed by the other program.

Satterlee, however, teaches **"providing means to present an alert to a user"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39), and **"providing means for the user to approve the one of the predetermined file system operations before being performed by the other program"** as "in step 605 the protector application 115 will consult the database 110 to determine if the user has been previously queried about the new non-validated executable file…If the user has previously approved the loading of this executable file in step 610, or if the user approves the new executable in this instance in step 615, then execution of the executable file will proceed" (Paragraph 45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 39, **McIchionc** and **Norton** do not explicitly teach a computer-readable medium comprising:

A) selecting the program for monitoring in response to the program not being on a safe list.

Satterlee, however, teaches **"selecting the program for monitoring in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs…If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 44, **McIchionc** and **Norton** do not explicitly teach a computer-readable medium comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations sending an alert in response to the program attempting to perform any predetermined file system operations.

Satterlee, however, teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "the behavior monitors 128 can take direct action to address a security threat or instruct the protector application 115 to query the user for instructions on how to handle the threat" (Paragraph 35) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **McIchionc's** and **Norton's** to provide a method to

allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

15. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Norton** (Article entitled "Norton AntiVirus Corporate Edition User's Guide, dated 09/11/2001) as applied to claims 2, 6, 8-9, 13-16, 21, 23-25, 28, 30, 32-34, 38, and 40-43 and further in view of **Satterlee et al.** (U.S. PGPUB 2004/0025015) as applied to claims 10-12, 17, 19-20, 22, 26, 29, 31, 35, 37, 39, and 44 and further in view of **Wolff et al.** (U.S. PGPUB 2002/0174358).

16. Regarding claim 18, **McIchionc**, **Norton**, and **Satterlee** do not explicitly teach a method comprising:

A) sending the alert to a network monitoring system.

Wolff, however, teaches **"sending the alert to a network monitoring system"** as "An event report, such as a virus detection event, is sent from a reporting computer 2 to a receiving computer 6 via an internet link 4" (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Wolff's** would have allowed **McIchionc's**, **Norton's**, and **Satterlee's** to provide a method to allow major antivirus software providers to accurately determine what viruses are common and attacking how many users in order to direct resources to combat these viruses, as noted by **Wolff** (Paragraph 4).

17. Claims 27 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McIchionc** (U.S. Patent 6,973,578) as applied to claim 1 and in view of **Norton** (Article entitled "Norton AntiVirus Corporate Edition User's Guide, dated 09/11/2001) as applied to claims 2, 6, 8-9, 13-16, 21, 23-25, 28, 30, 32-34, 38, and 40-43 and further in view of **Wolff et al.** (U.S. PGPUB 2002/0174358).

18. Regarding claim 27, **McIchionc** and **Norton**, do not explicitly teach a system comprising:

A) a network monitoring system; and

B) means to send an alert to the network monitoring system in response to flagging the other program.

Wolff, however, teaches **"a network monitoring system"** as "a receiving computer 6" (Abstract) and **"means to send an alert to the network monitoring system in response to flagging the other program"** as "An event report, such as a virus detection event, is sent from a reporting computer 2 to a receiving computer 6 via an internet link 4" (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Wolff's** would have allowed **McIchionc's** and **Norton's** to provide a method to allow major antivirus software providers to accurately determine what viruses are common and attacking how many users in order to direct resources to combat these viruses, as noted by **Wolff** (Paragraph 4).

Regarding claim 36, **McIchionc** and **Norton**, do not explicitly teach a method comprising:

A) providing a network monitoring system; and

B) providing means to send an alert to the network monitoring system in response to flagging the other program.

Wolff, however, teaches **"providing a network monitoring system"** as "a receiving computer 6" (Abstract) and **"providing means to send an alert to the network monitoring system in response to flagging the other program"** as "An event report, such as a virus detection event, is sent from a reporting computer 2 to a receiving computer 6 via an internet link 4" (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Wolff's would have allowed **McIchionc's** and **Norton's** to provide a method to allow major antivirus software providers to accurately determine what viruses are common and attacking how many users in order to direct resources to combat these viruses, as noted by **Wolff** (Paragraph 4).

Response to Arguments

19. Applicant's arguments filed on 11/08/2006 have been fully considered but they are not persuasive.

Applicant goes on to argue on page 13, that **"McIchionc does not teach or suggest allowing one of a highest security level, a middle security level and a lowest security level to be set"**. However, the examiner wishes to point to Column 2 of **McIchionc**, and refer to the third paragraph which states "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30). The examiner further wishes to point to Column 6 of **McIchionc**, and refer to the third and fourth paragraphs which state "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system...It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65). The examiner further wishes to state that the **McIchionc's** method clearly allows for the setting of varied levels of security for virus protection.

Applicant goes on to argue on page 13, that **"McIchionc does not teach or suggest flagging a program as being suspect or possibly containing a virus in response to at least one of the specific operations or set of conditions recited in claim 1"**. However, the examiner wishes to point to Columns 4-5 of **McIchionc**, which state "In order to facilitate the selection of the appropriate virus detection actions, each process may have an associated risk level identifier associated therewith...the process may be identified by...a method in which files are being accessed by the process (opened for read, opened for write, execution, etc.)" (Column 4, lines 62-67-Column 5, lines 1-13). The examiner further wishes to state that the **McIchionc's** method clearly

allows for the setting of varied levels of security for virus protection dependent on the identification of the actions being committed (see "write", "read", etc.).

Applicant goes on to argue on page 14, that **"Mclchionc also does not teach or suggest a particular security level being associated with each specific operation or set of operations"**. However, the examiner wishes to point to Columns 4-5 of **Mclchionc**, which state "In order to facilitate the selection of the appropriate virus detection actions, each process may have an associated risk level identifier associated therewith…the process may be identified by…a method in which files are being accessed by the process (opened for read, opened for write, execution, etc.)" (Column 4, lines 62-67-Column 5, lines 1-13). The examiner further wishes to state that the **Mclchionc's** method clearly allows for the setting of varied levels of security for virus protection dependent on the identification of the actions being committed (see "write", "read", etc.).

Applicant goes on to argue on page 14, that **"Mclchionc also does not teach or suggest flagging the program in response to occurrence of the specific recited operation or set of operations and the particular security level also being set that is associated with the specific operation or set of operations particular security level being associated with each specific operation or set of operations"**. However, the examiner wishes to point to Columns 4-5 of **Mclchionc**, which state "In order to facilitate the selection of the appropriate virus detection actions, each process may have an associated risk level identifier associated therewith…the process may be identified by…a method in which files are being accessed by the process (opened for read, opened for write, execution, etc.)" (Column 4, lines 62-67-Column 5, lines 1-13). The examiner further wishes to state that the **Mclchionc's** method clearly allows for the setting of varied levels of security for virus protection dependent on the identification of the actions being committed (see "write", "read", etc.).

Applicant goes on to argue on page 14, that **"Applicant respectfully submits that there is no teaching or suggestion in Mclchionc and Norton that their teachings be combined so as to provide the present invention as recited in the claims and such motivation only comes from Applicant's disclosure"**. In response

to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to configure the controller of Nilsen by applying the teachings of Subramanyam and Smith, III as indicated above, to enhance its performance. It would have been obvious to evaluate the information regarding the I/O operations to distribute the loads to the database server and to cache the information at the controller because Smith, III teaches that the I/O operations constitute a major portion of OLTP workload and thus caching the I/O operations would help avoid expensive disk accesses (Smith, III, col. 2, lines 30-32).

In response to applicant's argument on pages 4 and 6, *a prima facie case of obviousness* is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art. Once such a case is established, it is incumbent upon appellant to go forward with objective evidence of unobviousness. In re Fielder, 471 F.2d 640, 176 USPQ 300 (CCPA 1973).

Examiner is entitled to give claim limitations their broadest reasonable interpretation in light of the specification.

Interpretation of Claims-Broadest Reasonable Interpretation

During patent examination, the pending claims must be 'given the broadest reasonable interpretation consistent with the specification.' Applicant always has the opportunity to amend the claims during prosecution and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified. In re Prater, 162 USPQ 541,550-51 (CCPA 1969).

Reference is made to MPEP 2144.01 - Implicit Disclosure

"[I]n considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art

would reasonably be expected to draw therefrom." In re Preda, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)

Subsequent to an analysis of the claims it was revealed that a number of limitations recited in the claims belong in the prior art and thus encompassed and/or implicitly disclosed in the reference (s) applied and cited. It is logical for the examiner to focus on the limitations that are "crux of the invention" and not involve a lot of energy and time for the things that are not central to the invention, but peripheral. The examiner is aware of the duties to address each and every element of claims, however, it is also important that a person prosecuting a patent application before the Office or an stakeholders of patent granting process make effort to understand the level of one of ordinary skill in the (data processing) art or the level one of skilled in the (data processing) art, as encompassed by the applied and cited references. The administrative convenience derived from such a cooperation between the attorneys and examiners benefits the Office as well the patentee.

In view of the above, the examiner contends that all limitations as recited in the claims have been addressed in this Action.

For the above reasons, Examiner believed that rejection of the last Office action was proper.

In response to applicant's argument, to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

"Test of obviousness is not whether features of secondary reference may be bodily incorporated into primary reference's structure, nor whether claimed invention is expressly suggested in any one or all of references; rather, test is what combined teachings of references would have suggested to those of ordinary skill in art."

In re Keller, Terry, and Davies, 208 USPQ 871 (CCPA 1981).

"Reason, suggestion, or motivation to combine two or more prior art references in single invention may come from references themselves, from knowledge of those skilled in art that certain references or disclosures in references are known to be of interest in particular field, or from nature of problem to be solved;" Pro-Mold and Tool Co. v. Great Lakes Plastics Inc. U.S. Court of Appeals Federal Circuit 37 USPQ2d 1626 Decided February 7, 1996 Nos. 95-1171, -1181

"[q]uestion is whether there is something in prior art as whole to suggest desirability, and thus obviousness, of making combination." Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Company et al. U.S. Court of Appeals Federal Circuit 221 USPQ 481 Decided Mar. 21, 1984 No 83-1178.

Applicant goes on to argue on page 15, that **"Applicant respectfully submits that there is no teaching or suggestion in Mclchionc or Norton of allowing a security level to be set as provided by the present invention as recited in claim 9"**. However, the examiner wishes to point to Column 2 of **Mclchionc**, and refer to the third paragraph which states "varying levels of security may be employed based on the process that is opening the files" (Column 2, lines 29-30). The examiner further wishes to point to Column 6 of **Mclchionc**, and refer to the third and fourth paragraphs which state "The first and second categories thus ensure that security is heightened in those cases where it is needed. Further, the third and fourth categories prevent on-access scanning of too many files and interfering with the users of the system...It should be noted that the number of categories need not be set at four, and may include more or less based on the desires of the user" (Column 6, lines 55-65). The examiner further wishes to state that the **Mclchionc's** method clearly allows for the setting of varied levels of security for virus protection.

Applicant goes on to argue on page 15, that **"Applicant respectfully submits that Norton does not teach or suggest in this section of Norton or anywhere else in Norton about setting a level of security and following a predefined procedure in response to the level of security set"**. However, the examiner wishes to state that the limitation "setting a security level" is taught by **Mclchionc**, and only the "predefined procedure" is taught by **Norton**. The examiner further wishes to point to page 31 of

Norton which states "If you regularly scan the same set of files or folders you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus-free" (Page 31, Section: Configuring Custom Scans"). The examiner further wishes to state that it is clear that the custom scans of **Norton** allow for preset procedures on how and where to treat scans and located viruses.

Applicant goes on to argue on page 16, that **"Applicant respectfully submits that McIchionc does not teach or suggest the specific program operations recited in claim 15"**. However, the examiner wishes to point to Columns 4-5 of **McIchionc**, which state "In order to facilitate the selection of the appropriate virus detection actions, each process may have an associated risk level identifier associated therewith...the process may be identified by...a method in which files are being accessed by the process (opened for read, opened for write, execution, etc.)" (Column 4, lines 62-67-Column 5, lines 1-13). The examiner further wishes to state that the **McIchionc's** method clearly allows for the setting of varied levels of security for virus protection dependent on the identification of the actions being committed (see "write", "read", etc.).

Applicant goes on to argue on page 18, that **"Applicant respectfully submits that there is no teaching or suggestion in McIchionc and Satterlee that their teachings be combined so as to provide the present invention as recited in the claims in such motivation only comes from a reading of the present invention"**. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to configure the controller of Nilsen by applying the teachings of Subramanyam and Smith, III as indicated above, to enhance its performance. It would have been obvious

to evaluate the information regarding the I/O operations to distribute the loads to the database server and to cache the information at the controller because Smith, III teaches that the I/O operations constitute a major portion of OLTP workload and thus caching the I/O operations would help avoid expensive disk accesses (Smith, III, col. 2, lines 30-32).

In response to applicant's argument on pages 4 and 6, *a prima facie case of obviousness* is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art. Once such a case is established, it is incumbent upon appellant to go forward with objective evidence of unobviousness. In re Fielder, 471 F.2d 640, 176 USPQ 300 (CCPA 1973).

Examiner is entitled to give claim limitations their broadest reasonable interpretation in light of the specification.

Interpretation of Claims-Broadest Reasonable Interpretation

During patent examination, the pending claims must be 'given the broadest reasonable interpretation consistent with the specification.' Applicant always has the opportunity to amend the claims during prosecution and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified. In re Prater, 162 USPQ 541,550-51 (CCPA 1969).

Reference is made to MPEP 2144.01 - Implicit Disclosure

"[I]n considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom." In re Preda, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)

Subsequent to an analysis of the claims it was revealed that a number of limitations recited in the claims belong in the prior art and thus encompassed and/or implicitly disclosed in the reference (s) applied and cited. It is logical for the examiner to focus on the limitations that are "crux of the invention" and not involve a lot of energy and time for the things that are not central to the invention, but peripheral. The examiner is aware of the duties to address each and every element of claims, however, it is also important that a person prosecuting a patent application before the Office or an

stakeholders of patent granting process make effort to understand the level of one of ordinary skill in the (data processing) art or the level one of skilled in the (data processing) art, as encompassed by the applied and cited references. The administrative convenience derived from such a cooperation between the attorneys and examiners benefits the Office as well the patentee.

In view of the above, the examiner contends that all limitations as recited in the claims have been addressed in this Action.

For the above reasons, Examiner believed that rejection of the last Office action was proper.

In response to applicant's argument, to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

"Test of obviousness is not whether features of secondary reference may be bodily incorporated into primary reference's structure, nor whether claimed invention is expressly suggested in any one or all of references; rather, test is what combined teachings of references would have suggested to those of ordinary skill in art."

In re Keller, Terry, and Davies, 208 USPQ 871 (CCPA 1981).

"Reason, suggestion, or motivation to combine two or more prior art references in single invention may come from references themselves, from knowledge of those skilled in art that certain references or disclosures in references are known to be of interest in particular field, or from nature of problem to be solved;" Pro-Mold and Tool Co. v. Great Lakes Plastics Inc. U.S. Court of Appeals Federal Circuit 37 USPQ2d 1626 Decided February 7, 1996 Nos. 95-1171, -1181

"[q]uestion is whether there is something in prior art as whole to suggest desirability, and thus obviousness, of making combination." Lindemann Maschinenfabrik GMBH v.

American Hoist and Derrick Company et al. U.S. Court of Appeals Federal Circuit 221 USPQ 481 Decided Mar. 21, 1984 No 83-1178.

Applicant goes on to argue on page 19, that **"Applicant respectfully submits that there is no teaching or suggestion in McIchionc and Wolff that their teachings be combined so as to provide the present invention as recited in the claims in such motivation only comes from a reading of the present application"**. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to configure the controller of Nilsen by applying the teachings of Subramanyam and Smith, III as indicated above, to enhance its performance. It would have been obvious to evaluate the information regarding the I/O operations to distribute the loads to the database server and to cache the information at the controller because Smith, III teaches that the I/O operations constitute a major portion of OLTP workload and thus caching the I/O operations would help avoid expensive disk accesses (Smith, III, col. 2, lines 30-32).

In response to applicant's argument on pages 4 and 6, *a prima facie case of obviousness* is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art. Once such a case is established, it is incumbent upon appellant to go forward with objective evidence of unobviousness. In re Fielder, 471 F.2d 640, 176 USPQ 300 (CCPA 1973).

Examiner is entitled to give claim limitations their broadest reasonable interpretation in light of the specification.

Interpretation of Claims-Broadest Reasonable Interpretation

During patent examination, the pending claims must be 'given the broadest reasonable interpretation consistent with the specification.' Applicant always has the opportunity to amend the claims during prosecution and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified. In re Prater, 162 USPQ 541,550-51 (CCPA 1969).

Reference is made to MPEP 2144.01 - Implicit Disclosure

"[I]n considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom." In re Preda, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)

Subsequent to an analysis of the claims it was revealed that a number of limitations recited in the claims belong in the prior art and thus encompassed and/or implicitly disclosed in the reference (s) applied and cited. It is logical for the examiner to focus on the limitations that are "crux of the invention" and not involve a lot of energy and time for the things that are not central to the invention, but peripheral. The examiner is aware of the duties to address each and every element of claims, however, it is also important that a person prosecuting a patent application before the Office or an stakeholders of patent granting process make effort to understand the level of one of ordinary skill in the (data processing) art or the level one of skilled in the (data processing) art, as encompassed by the applied and cited references. The administrative convenience derived from such a cooperation between the attorneys and examiners benefits the Office as well the patentee.

In view of the above, the examiner contends that all limitations as recited in the claims have been addressed in this Action.

For the above reasons, Examiner believed that rejection of the last Office action was proper.

In response to applicant's argument, to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves

or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

"Test of obviousness is not whether features of secondary reference may be bodily incorporated into primary reference's structure, nor whether claimed invention is expressly suggested in any one or all of references; rather, test is what combined teachings of references would have suggested to those of ordinary skill in art."

In re Keller, Terry, and Davies, 208 USPQ 871 (CCPA 1981).

"Reason, suggestion, or motivation to combine two or more prior art references in single invention may come from references themselves, from knowledge of those skilled in art that certain references or disclosures in references are known to be of interest in particular field, or from nature of problem to be solved;" Pro-Mold and Tool Co. v. Great Lakes Plastics Inc. U.S. Court of Appeals Federal Circuit 37 USPQ2d 1626 Decided February 7, 1996 Nos. 95-1171, -1181

"[q]uestion is whether there is something in prior art as whole to suggest desirability, and thus obviousness, of making combination." Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Company et al. U.S. Court of Appeals Federal Circuit 221 USPQ 481 Decided Mar. 21, 1984 No 83-1178.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,886,099 issued to **Smithson et al.** on 26 April 2005. The subject matter disclosed therein is pertinent to that of claims 1-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,735,700 issued to **Flint et al.** on 11 May 2004. The subject matter disclosed therein is pertinent to that of claims 1-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0116639issued to **Chefalas et al.** on 22 August 2002. The subject matter disclosed therein is pertinent to that of claims 1-44 (e.g., methods to provide virus protection on computers).

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi
Patent Examiner

TIM VO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

January 11, 2007

Leslie Wong LW

Primary Examiner